

4 tips for implementing GDPR compliance in a way that delivers commercial value

The clock is ticking for GDPR compliance. There is mounting pressure to deliver a GDPR strategy that not only mitigates the risks of non-compliance, but balances the need for stand-out customer relationships and long-term business objectives.

Balance compliance with business growth

Underlying the implementation of the GDPR is an organisation-wide behavioural change. While there are many upsides to the changes required under GDPR, such as clearer reporting and data storage, GDPR compliance will inevitably necessitate changes in practices that staff (and customers) are not used to.

For instance, under GDPR the consent process is more stringent. Simply shoe-horning in a more thorough consent process may be interpreted as an added level of bureaucracy, or an extra layer of paper work, which may affect business-as-usual and subsequently the acquisition of and retention of policies.

The real business challenge then is to seamlessly integrate the requirements of the GDPR – including consent – into business processes in such a way that doesn't provide any additional burden to either staff or customers.

The overarching objectives of the business must be kept front-mind, says David Nottingham, Head of Marketing Strategy, Wesleyan.

“It's important that GDPR implementation does not lose sight of the customer; the risk is that businesses become regulation-driven rather than driven by the end customer and its commercial goals.”

It's therefore a balancing act; strategising around GDPR must consider compliance in way that doesn't impede business as usual, stifle innovation, or inhibit growth.



Use legitimate interest (but don't rely upon it)

There is still some confusion and trepidation among insurers around the guidance offered by the Information Commissioners Office (ICO). But in fact, the industry's current best practice (with some less onerous updates to the data strategy and consent process) are likely to be enough for marketing practices to fall into line. As such, the GDPR needn't be the huge headache for marketers that it's often perceived to be.

The GDPR sets out a number of legal basis for processing personal data. One of these states that data processing is lawful if 'necessary for the purposes of legitimate interests.' Yasmin Durrani, Data Protection Officer, Swiss Re explains:

“After May 25 (GDPR deadline day) business may solicit customers to update their preferences under legitimate interest.”

This recital on legitimate interest is a big relief for the customer-focused marketers and for GDPR project managers with a focus on long term business growth.

The big question then: When and where should legitimate interest be used? Marketing is of course a legitimate interest and insurance businesses won't be required to obtain fresh consent from individuals where 'the standard of consent meets the new requirements under the GDPR.' In other words, using personal data to power marketing efforts shouldn't be a problem if you have already communicated with the consumer in the right way.

However, the legitimate interest argument will not save marketers completely from the consent conundrum. While the GDPR does indeed provide for 'legitimate interest' as a legal basis for using personal data without obtaining consent, marketers mustn't be lured into thinking they will not have to ask people permission to use their personal data.

A 'legitimate interest' must benefit a single company, or society as a whole, and can be derived from processing personal data in a lawful way; Merely having a legitimate interest does not equal an entitlement to use personal data. As David Nottingham, Head of Marketing Strategy, Wesleyan says:

“Legitimate interest can't be used as a catch-all policy or an excuse for businesses to maintain practices or procedures. Instead, it should be used sensibly for the benefit of the customer in the right circumstances.”

Anonymising data can help
Personal data - Any information relating to an identifiable natural person.
Identifiable - One who can be identified directly or indirectly, in particular by a reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, psychological, genetic, mental, economical, cultural, or social identity of that person.

How can anonymised data help to navigate the risk of holding and processing personal data?

From an operational standpoint, it's difficult to integrate the GDPR consent requirements in a way that doesn't disrupt business-as-usual. Considering this, many insurers aim to reduce the need for consents by anonymising data to make it personally unidentifiable. Anonymisation being the process of turning data into a form which does not identify individuals or where identification is not likely to take place.

Anonymised data is therefore not personal. In turn, the approach de-risks potential for data breaches (and the associated fines, reputational damage etc.). Ultimately, the principles of data protection do not apply to anonymous information because it is managed in a way that ensures the data subject is no longer identifiable.

But, like the 'legitimate interest' caveat, insurers must not be lured into believing anonymisation is a quick fix.

Given the mass of personal information available online in the digital age, the opportunity to ensure data is 100% anonymised is a tough task. Anonymisation is a useful tool, but is not a silver bullet that insurers can use to eliminate the GDPR compliance burden.

GDPR is a catalyst for innovation

Throughout we have highlighted the importance of implementing GDPR compliance in a way that marries with the long term commercial objectives of the business. But equally, insurers should be looking to leverage GDPR as a catalyst for innovation and a framework to drive greater commercial value.

Despite the perception that the insurance industry is risk-averse and slow to adopt digital transformation (in comparison to fintech say), traditional insurers are now starting to make digital leaps amid a need to innovate on a long-standing model.

In short, the insurance industry faces conflicting challenges: Exponentially increasing amounts of data versus a more stringent regulatory landscape. Many see restrictive data regulation as having a detrimental impact on the insurance industry, inhibiting data collection and processing activities as well as adding to the compliance burden.

However, underlying the regulation is the fair and transparent use of customer data. In an age of stagnating premium growth, insurers must look for new ways to drive customer loyalty and acquisition. GDPR, and the level of transparency it introduces, can be the vehicle to establish greater consumer trust and enable growth.

David Nottingham, Head of Marketing Strategy, Wesleyan sees GDPR as a catalyst for a greater focus on data, technology and customer insight. He says:

“In light of the GDPR, technology must be joined up in all areas, from contact centres to marketing teams. At every touchpoint insurance businesses must be aware of where the customer is in the conversation. This is where CRM plays a vital role in creating a single view of the customer.”

In this way, rethinking the value exchange to strengthen customer relationships, and harnessing the power of data to enrich customer conversations can serve to enable much needed innovation.



“Technology and data enabled insurance customer journeys will see differentiation that is increasingly based on quality customer service as opposed to price. Insurers that implement GDPR reforms to optimise customer journeys in this way will win out in the long run,” says Nottingham.



Leverage transparency to build customer trust

Historically, the immensely valuable commodity of personal data has been acquired for a fraction of its worth. For years, personal data has been used for undisclosed purposes, and with no legal obligation to reveal its providence.

But the GDPR is a giant step towards a more transparent and efficient data economy. In relation to customer engagement, the new regulation will have a positive impact on the quality of data used and subsequently the quality of the customer experience, including more precise targeting, pricing and underwriting.

Transparency helps to navigate the fine line between ‘creepy’ and ‘relevant’. This is of vital importance because any underlying sense of creepiness ultimately causes a lack of trust. The resulting trust issues increase the chances of consumers falsifying and misrepresent information*.

The trend towards the falsification of information is particularly detrimental for insurance businesses that require accurate information for personalising communications and customising product offers. For insurers, who rely heavily on a rich vein of personal data, any moves towards strengthening data quality and customer trust must be welcomed.

**<https://www.marketingweek.com/2015/07/08/consumers-are-dirtying-databases-with-false-details/>*

Final thoughts

It is imperative that compliance remains a top priority for the insurance industry. But can the industry truly maintain compliance and business growth as the market begins to heat-up?

Success lies in recognising that compliance and delivering commercial growth are not mutually exclusive, but in fact go hand-in-hand. While there may be some short-term hurdles to overcome, difficult processes to change and stubborn people to convince, the benefits of transparent and better data management far outweigh the costs.

It's important to remember that GDPR compliance must not simply be delivered in a tick-box fashion, but built in a way that delivers on your commercial model. This is the balancing act; whoever plays it best will come out strongest.



How Hitachi Solutions can give you the edge?

Are you struggling to manage complex and numerous legacy systems? Are you juggling data in order to piece together a fragmented view of your customer? Are your systems providing everything needed for explicit consent? Does your technology allow for subject access requests and seamless data portability?

Hitachi Solutions work within the insurance sector to find innovative and effective ways to unite complex silos of information. Hitachi Solutions enable GDPR compliance with a 360° view of the customer. Through uniting what is very often a compartmentalised structure, our systems work to eradicate inefficiency and ensure compliance. From policy admin to claims management, we work to improve processes, add value and build customer loyalty.



Hitachi Solutions



Microsoft

Dynamics 365